

How to setup logging in DSR series

Step1: Make sure the rule that you want to log is enable, we use the firewall rule for example. In the **Log** field, make sure your select **Always**.

The screenshot shows the 'Firewall Rule Configuration' page. The 'Log' field is highlighted with a red box and set to 'Always'. Below it, the 'QoS Priority' is set to 'Normal-Service'. The 'Source NAT Settings' section shows 'External IP Address' as 'WAN interface Address', 'Single IP Address' as empty, and 'WAN Interface' as 'WAN1'. The 'Destination NAT Settings' section shows 'Internal IP Address' as '192.168.10.10', 'Enable Port Forwarding' checked, and 'Translate Port Number' as '80'.

Field	Value
From Zone	INSECURE (WAN)
To Zone	SECURE (LAN)
Service	HTTP
Action	Always Allow
Select Schedule	
Source Hosts	Any
From	
To	
Destination Hosts	Any
From	
To	
Log	Always
QoS Priority	Normal-Service
External IP Address	WAN interface Address
Single IP Address	
WAN Interface	WAN1
Internal IP Address	192.168.10.10
Enable Port Forwarding	<input checked="" type="checkbox"/>
Translate Port Number	80

Step 2. Under the **TOOLS->Log Settings-> LOG CONFIGURATION**, select the direction and dropped/accesspt packet you want to log.

DSR-500N // SETUP ADVANCED **TOOLS** STATUS HELP

Admin Date and Time **Log Settings** System Firmware Firmware via USB Dynamic DNS System Check Schedules

LOGS CONFIGURATION LOGOUT

This page allows user to configure system wide log settings.

Save Settings Don't Save Settings

Routing Logs

	Accepted Packets	Dropped Packets
LAN to WAN:	<input type="checkbox"/>	<input type="checkbox"/>
WAN to LAN:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>
DMZ to WAN:	<input type="checkbox"/>	<input type="checkbox"/>
LAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>
DMZ to LAN:	<input type="checkbox"/>	<input type="checkbox"/>

System Logs

All Unicast Traffic:

All Broadcast / Multicast Traffic:

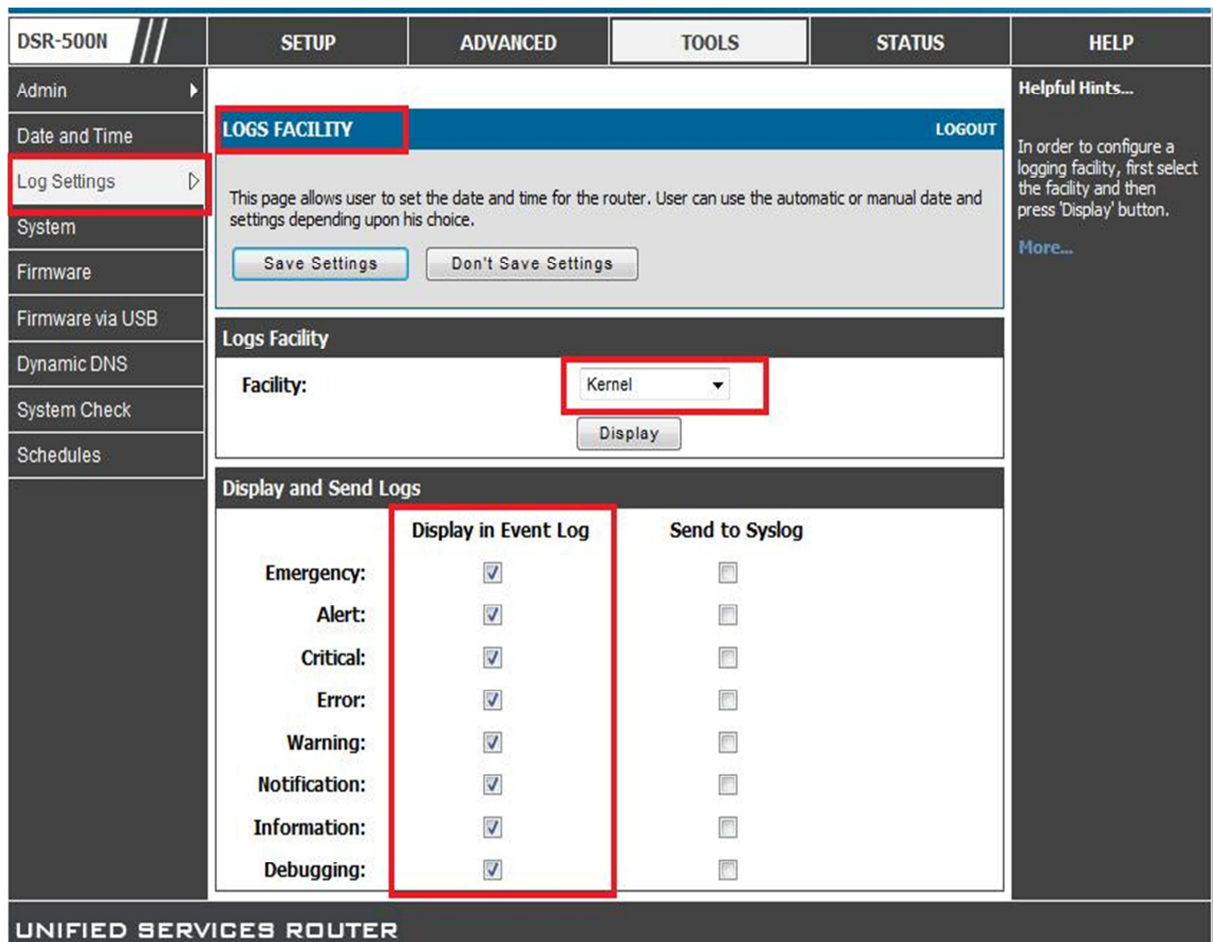
Other Events Logs

Bandwidth Limit:

Helpful Hints... Traffic through each network segment (LAN, WAN, DMZ) can be tracked based on whether the packet was accepted or dropped by the firewall. Denial of service attacks, general attack information, login attempts, dropped packets, and similar events can be captured for review by the IT administrator. More...

UNIFIED SERVICES ROUTER

Step3:Under **TOOLS**->**Log Settings**-> **LOGS FACILITY**, select the Log Facility and the severity of log want to displays.



You can refer the following for more detail:

Logs Facility:

Facility: There are three core components to the router's firmware and the granularity of logging within each can be set independently. Choose between Kernel, System, and Local-0 Wireless.

Kernel: This covers log messages that correspond to the Linux kernel such as logs generated by firewall or network stack traffic.

System: This covers application and management level features such as SSL VPN or administrator changes for managing the unit.

Display and Send Logs

Each of the following type of logs can be sent to the **Event Log** viewer in the GUI and/or the **Syslog server** configured to capture remote logging.

When a particular severity level is selected, all events with severity equal to and greater than the chosen severity are captured. The severity levels available for logging are:

- EMERGENCY: system is unusable
- ALERT: action must be taken immediately
- CRITICAL: critical conditions
- ERROR: error conditions
- WARNING: warning conditions
- NOTIFICATION: normal but significant condition
- INFORMATION: informational
- DEBUGGING: debug-level messages